# Comparative Analysis of Static & Dynamic Probabilistic Risk Assessment

Christopher J. Mattenberger, Science and Technology Corporation, NASA Ames Research Center
Donovan L. Mathias, NASA Ames Research Center
Susie Go, NASA Ames Research Center

Key Words: Dynamic PRA, Risk-Informed Design, Space Exploration, Crewed Spacecraft

*SUMMARY & CONCLUSIONS*

This study examines three different methodologies for producing loss-of-mission (LOM) and loss-of-crew (LOC) risks estimates for probabilistic risk assessments (PRA) of crewed spacecraft. The three bottom-up, component-based PRA approaches examined are a traditional static fault-tree, a fault-tree hybrid, and a dynamic Monte Carlo simulation. These approaches were used to model a generic reaction control system thruster pod of a crewed spacecraft and mission, and a comparative analysis of the methods is presented.

The methods are assessed in terms of the process of modeling a system, the actionable information produced for the design team, and the overall fidelity of the quantitative risk evaluation generated. The process of modeling a system is compared in terms of the effort required to generate the initial model, to update the model in response to design changes, and to support mass-versus-risk trade studies. The results are compared by examining the top-level LOM/LOC estimates and the relative risk driver rankings at the failure mode level. The fidelity of each modeling methodology is discussed in terms of its capability to handle real-world system dynamics such as cold-sparing, changes in mission operations due to loss of redundancy, and common cause failure modes.

The paper also discusses the applicability of each methodology to the different phases of system development and shows that a single methodology may not be suitable for all of the many purposes and goals of a spacecraft PRA. A design process that follows a risk-informed design paradigm must have quantitative insight into the relative risks facing the system in order to balance the requirements placed upon the performance, mass, cost, and risk [2]. To arrive at a final design of a complex space system that is likely to meet all constraints, these requirements must be understood and traded against each other as early as the conceptual design phase in order to avoid costly re-designs or project cancellation [13]. During the conceptual design phase, the assessment methodology selected needs to respond rapidly to a changing design and provide accurate relative risk drivers with limited design detail. The fault-tree hybrid approach is shown to be best suited to these early assessment needs. As the design begins to mature, more precise insights are required to accurately discriminate between similar trade study options and identify the ones that can reduce overall risk most efficiently. To accomplish this, the level of design detail represented in the risk model must go beyond redundancy and nominal mission operations to include dynamic, time- and state-dependent system responses as well as diverse system capabilities. This is best accomplished using the dynamic simulation approach, since these phenomena are not easily captured by static methods. Ultimately, once the design has been finalized and the goal of the PRA is to provide design validation and requirement verification, more traditional, static fault-tree approaches may become as appropriate as the simulation method.

## *1 INTRODUCTION*

Implementation of risk-informed design allows the design team to balance the demands upon the system by considering risk on a co-equal basis with more traditional constraints such as mass, performance and cost [2]. Depending on the phase of the project life cycle and the goals of the risk analysis, various PRA methodologies could be used to produce quantitative risk estimates to enable such a process.

In order to better understand the applicability various PRA methodologies, a comparative analysis has been performed using a generic reaction control system (RCS) thruster pod and mission [1] as a basis to elucidate the advantages and disadvantages of each methodology.

The nominal mission under consideration is that of a crewed spacecraft visiting the International Space Station (ISS). The spacecraft is launched into orbit and then must utilize its onboard propulsion and RCS to rendezvous and dock with ISS 24 hours after launch. Once docked, the spacecraft remains on orbit for 210 days while the RCS is relatively quiescent. Once the spacecraft has completed its stay at ISS, or in the event of an abort from orbit, the spacecraft must once again utilizes its propulsion and RCS to perform de-orbit, entry, descent and landing operations to return the crew safely within 4.5 hours.

The RCS thruster pod considered consists of two groups of three thrusters. Loss of any two thrusters in the same group

triggers an abort from orbit and ends the nominal mission, thus producing loss-of-mission (LOM), and the loss of an entire group triggers a loss-of-crew (LOC). A simplified schematic of this system is shown in Figure 1 with thrusters represented as blue triangles and isolation valves represented as blue boxes. The nominal operation of the system calls for "stand by" operation, with Thruster A to be fired until it experiences a failure, then Thruster B is fired until failure, and finally Thruster C would then be used to return the crew safely.

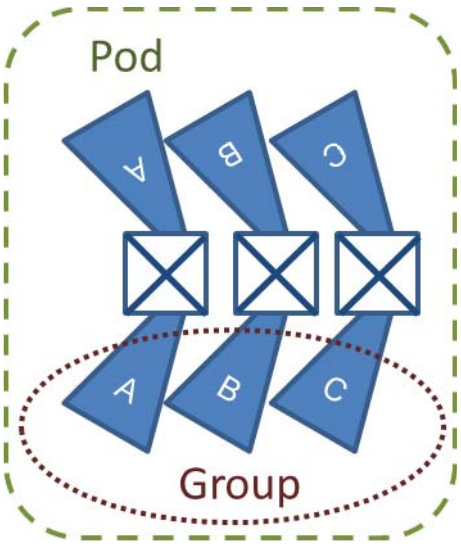



*Figure 1 – RCS Thruster Pod Configuration*

Each thruster consists of a fuel valve, an oxidizer valve, and an exciter. The valves failure modes consist of fails to open on demand, fails to close on demand, fails operationally while firing, and fails leaky over time. The exciter can fail off when powered on. The failure rate data is summarized in Table 1. These failure rates are from tables provided in the Institute of Electrical and Electronics Engineers reliability data book [3].

Each fuel and oxidizer valve is backed up by an isolation valve, which is shared between two thrusters in different groups. The isolation valve is nominally open and only closes if one of two downstream valves has failed open or leaky. If the isolation valve fails to close or leaks, then a LOC is assumed to occur immediately. If the isolation valve successfully closes, then both downstream thrusters are deselected for the rest of the mission and the isolation valve must not leak in order to avoid LOC while crewed or loss-of-vehicle (LOV) while docked to ISS.

| Failure Mode | Failure Rate / Probability |
|---|---|
| Valve – Fails to Open | 2.05e-6 / demand |
| Valve – Fails to Close | 1.51e-6 / demand |
| Valve – Fails Operationally | 9.00e-7 / hour |
| Valve – Fails Leaky | 5.00e-8 / hour |
| Exciter – Fails Off | 1.69e-5 / hour |

*Table 1 – Failure Rate Data*

Table 2 summarizes the risk exposure times and demands by mission phase for each thruster group in the pod. It is important to note that only the currently selected thruster is demanded to fire, while all other thrusters only accrue risk of Valve – Fails Leaky. This leads to uncertainty about how many demands and how much firing time will be accrued by each individual thruster in this cold-spare configuration during an actual mission.

| Failure Mode | Pre-Docking | Docked | Post-Undock |
|---|---|---|---|
| Valve – Fails to Open | 2,000 demands | N/A | 1,000 demands |
| Valve – Fails to Close | 2,000 demands | N/A | 1,000 demands |
| Valve – Fails Operationally | 2 hours | N/A | 1 hours |
| Valve – Fails Leaky | 24 hours | 5040 hours | 4.5 hours |
| Exciter – Fails Off | 24 hours | N/A | 4.5 hours |

*Table 2 – Risk Exposure by Mission Phase*

Table 3 gives the common cause factor (CCF) values that were used for the RCS thrusters. These CCFs are based upon the Global Alpha Modeling Tool (GAMUT) [2] developed at NASA Johnson Space Center, which is based upon NUREG/CR-5485 [14] and NUREG/CR-5496 [15]. The values take into account an assumed staggered testing scheme where components are periodically inspected for indications of incipient failure modes and that these are demand-type components.

| Common Cause Group Size | Common Cause Factor |
|---|---|
| CCF of 2 of 3 | 0.04830 |
| CCF of 3 of 3 | 0.00517 |

*Table 3 – Common Cause Failure Conditional Probabilities*

## *2 METHODOLOGIES*

The fidelity of each modeling methodology is discussed in terms of its capability to handle the real-world system dynamics such as cold-sparing, changes in mission operations and system topology due to loss of redundancy, as well as common cause failure modes. Despite the common set of assumptions about concept of operation, risk exposure, and failure rates presented in Section 1, each method must make additional assumptions in order to produce a risk estimate. As such, each methodology provides a risk estimate for an approximate problem. The degree of the approximation versus the cost of obtaining the solution, in terms of risk analyst effort and time, is of key interest in determining the value provided to the design team. This value is a function of the stage of system development, design details available, and desired risk insights to be obtained. These factors are also discussed for each of the modeling approaches.

### 2.1 *Static Fault-Tree Approach*

This approach utilized SAPHIRE 8 [5], developed at the Idaho National Laboratory, to construct a static fault-tree to capture the risk of the RCS thruster system. Multiple instances of the fault-tree were constructed to capture the various LOM and LOC end states, as a single model cannot capture both. Having multiple models of the same system can prove difficult to manage if the design is rapidly evolving, the turnaround time for performing trade studies is fast, or the inputs are in flux.

The fault-tree basic events were calculated off-line and loaded into the model. A major assumption that must be made is determining how many demands each thruster must undertake successfully. Conservatively, it could be assumed that each thruster in a group must fire all 3,000 demands of the mission. However, this excessive conservatism produces unrealistically high risk estimates results that are not useful. Optimistically, it has been assumed that all three thrusters in a group each fire an equal amount. The true dynamic reallocation of firings after a thruster failure cannot be accounted for easily in a fault-tree. Similarly, incorporating dynamic reallocation of the firing and leakage times is also difficult. For example, an isolation valve should only begin to accrue leakage risk after a random thruster valve failure, but because the time of this failure is uncertain, the model must conservatively assume that the isolation valve must not leak for the entire mission duration.

Moreover, the real-world reason to abort the nominal mission once the vehicle has become zero fault tolerant to LOC is to reduce the risk exposure to the crew and maximize the chance of returning them safely. However, the fault-tree approach does not allow for an elegant method of accounting for time-varying abort criteria in the results. In order to more accurately capture the time- and state-dependence of system functionalities and behaviors like dynamic reallocation of demands and aborts from orbit, an intractable number of event trees and corresponding fault-trees would need to be constructed. This would make the assessment prohibitively costly and unable to keep up with a rapidly evolving conceptual or preliminary design. However, using this type of method with a long development lead-time and conservative assumptions may be completely appropriate later in the critical design phase when the design has stabilized and the purpose of the assessment is to verify that it meets a risk requirement.

Common cause failure modes are captured only when they would result directly in a LOM or LOC depending upon the end-state of the model. Thus, the model does not take into account mixed cases of both random and common cause failure modes combining to cause LOC.

After the model is created, it must be solved using a specific method in the SAPHIRE program. Both the results and the computation time can vary widely, depending on the chosen solver method and the number of cutsets the solver method produces. The cutsets capture all of the approximate model's possible failure modes and their calculated value deterministically, yielding an incredible amount of data that must be processed in order to provide actionable information to decision makers.

Overall, this method produces a very precise solution, but to a very approximate problem. It is extremely useful for rigorously capturing all potential failure modes of the approximate problem, but suffers from a lack of responsiveness, which can be a determinate in rapidly evolving designs.

### *2.2 Rapid Fault-Tree Hybrid Approach*

This approach utilizes the Ames Reliability Tool (ART), an Excel-based, implicit event-tree/fault-tree generator developed at NASA Ames Research Center based upon previous work [6]. The ART model deterministically produces estimates of LOM and LOC, focusing on risk-driving cutsets, which are expected to be those driven by common cause failure modes.

The ART model has the ability to capture dynamic reallocation of demands after failure by using well-known 'cold spare' or stand-by unit redundancy calculations [8]. This method is also able to capture the dynamic change in mission duration if an abort is triggered, and accurately captures the reduction in crew risk in the case of a degraded vehicle state. Additionally, only one model of the system needs to be built, as the ART is able to produce both LOM and LOC estimates from the same model with an extremely simple set of input fields. This method utilizes the built-in functionality of the ART to rapidly create models, enabling the risk analyst to work in real-time with designers.

One limitation of this method is that, the ART is not able to handle all potential redundancy configurations and does not take into account cross-cutting failure modes between different types of components or different failure modes within a set of similar components. As such, this method does not account for cascade failure modes where a thruster failing open in one group propagates to deselect the corresponding thruster in the other group due to activation of the isolation valve. Furthermore, the ART model does not capture thruster loss due to combinations of failure modes, i.e., when one thruster fails to open while another thruster fails to close.

However, the model is able to capture combinatorial mixed cases of both random failures and common cause failures within a specific failure mode or component. Depending on the system's risk-driving failure modes, optimistically omitting these cutsets may or may not impact the overall results, as these cutsets contain only random failures, which are often lower probability than those containing common cause failures. Moreover, if the purpose of the risk assessment is to compare two competing designs, then it is conceivable that these failure modes will not be a difference that makes a difference in the design trade study.

This method sacrifices precision in the estimate in order to respond more rapidly to the needs of the decision makers by providing relative risk estimates that capture the system's key dynamics along with accurate relative rankings of the risk drivers. This allows the risk analyst to quickly produce a range of estimates based upon uncertain input data and determine the

sensitivity of the estimate to the lack of design knowledge.

### *2.3 Dynamic Monte Carlo Simulation Approach*

This approach utilizes commercially available Monte Carlo style simulation software called GoldSim [7]. The risk analyst must create an entirely new model, tailored to the specific design details of the system at hand. The approach seeks to include all dynamic interactions and dependencies between all components and failure modes, but at the cost of model complexity, model validation challenges and, ultimately, in run-time, depending on the number of realizations required to achieve the desired level of confidence in the reliability estimate.

The models produced with this methodology have the ability to not only produce estimates of LOM and LOC, but also to produce estimates of LOV or crew-stranding at ISS. They can also provide scenario-based event timing information and data on successful missions or degraded vehicle states that do not trigger LOC, LOV, or LOM. These results can provide decision makers with great insight into maintenance concerns or the value of repair capability.

In addition, unlike a traditional fault-tree, the dynamic approach is able to handle more complex and often more representative graph-like connections that occur in many space systems. The Monte Carlo approach inherently allows dynamic reallocation of demands and changes in system topology that may occur after failure. Common cause failure modes can be gracefully introduced into the model framework, which allows for complete simulation of the Multiple Greek Letter (MGL) [14] method. This allows common cause failures to be accounted for within any subset of the component group and not just failures of the entire group.

Overall, this method most accurately captures the behavior of the systems and yields the greatest design insights, but comes at the cost of greatly increased model complexity. This complexity reduces the model's ability to rapidly respond to an evolving design, makes debugging extremely challenging, increases computational run-times as the model grows. These factors can make the approach too costly to effectively support risk-informed design in early stages of development. However, recent advancements in cloud computing [9] and supercomputing [10] are reducing the time required to produce risk estimates at the desired confidence level and may enable these complex analysis techniques to become advantageous earlier in the design cycle.

## *3 RESULTS*

System-level LOM and LOC estimates are presented along with rankings of system risk-drivers by failure mode. In addition, other meaningful model outputs produced by the dynamic simulation method, but not provided by the fault-tree or hybrid approach, are discussed. The ability of each method to provide actionable information for decision support is also explored.

### *3.1 System-Level Risk Estimates*

LOM and LOC results are presented below in Figure 2. As expected, the hybrid model predicts lower risk than the simulation methodology due to the known limitations of the model, which does not account for cross-failure or cross-component system failure modes. The hybrid model captures the majority of the LOM and LOC risk, which stems from CCF modes. The fault-tree results were calculated with both the 'Min-Cut' and 'BDD' solvers, which produced numerical results that differed by 2%. The fault-tree results are lower than those of the other methods due to the optimistic assumption about the duty cycle for each thruster necessitated by the inability to capture dynamic demand reallocation. Such an approach does not take into account the additional demands other thrusters must undertake to make-up for those of a failed group member. Contrarily, conservatively neglecting to include dynamic abort modes in the fault-tree has caused an increase in LOC risk. The dynamic approach results were obtained running 100,000 Monte Carlo simulations over a period of 11 hours on a quad-core Intel i5 processor. Determining the proper number of realizations is important to achieving converged results at the desired level of confidence. Producing high-fidelity results that capture all possible component connectivity and dynamic reallocation of RCS demands would require a prohibitive number of realizations. However, this degree of fidelity is not necessary to capture a converged estimate at the system level.

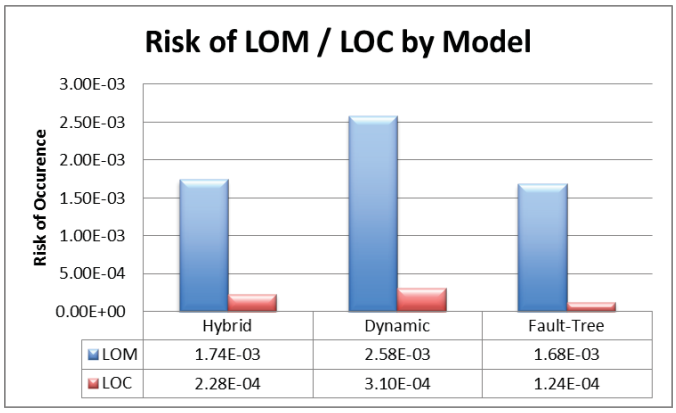



*Figure 2 – System-Level LOM/LOC Results by Model*

All of the methods considered can produce a top-level estimate of LOM and LOC. However, both the hybrid and fault-tree approach must make many assumptions to approximate the real-world system and, thus, underestimate LOM by 33% and 35%, respectively, and LOC by 26% and 60%, respectively. Depending on the degree of dynamics and graph-like component interactions, such assumptions could introduce so much uncertainty into the results that the actionable information provided to the decision maker is minimal. If the omissions in modeling fidelity drive the risk of the system, then the results cannot be trusted on an absolute scale and relative risk results between competing design options cannot be utilized

A major benefit of the simulation method is that it also records the time at which failure occurs. Such information can be extremely useful if the consequences of failure are time-

and state-dependent, like during an ascent to orbit on a failing launch vehicle [11] or if increased time on orbit would enable additional scientific research and increased availability of the ISS. In particular, accounting for the temporal relations of failure initiators allows failures that occur while docked to ISS to be counted as LOV instead of LOC. The dynamic results can provide insight into degraded system states that do not lead to a LOM, but simply to a loss of redundancy and a continuation of the nominal mission. Such results can provide insights into expected observed component failure frequencies and aid in determining repair capabilities and maintenance schedules.

### *3.2 System Risk Drivers*

Point estimates of system-level risk can be useful for comparing two different design options or determining if a design meets requirements. However, during the conceptual and preliminary phases of system development, insights into the system's current risk drivers can provide designers with valuable guidance and feedback on how to most effectively increase system reliability and safety.

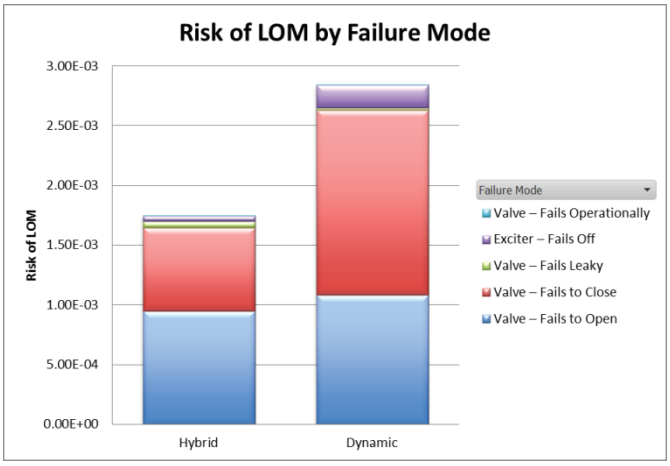



*Figure 4 – System Risk of LOM by Failure Mode for the Hybrid and Dynamic Methods*

LOM Results at the thruster failure mode level are provided in Figure 4 for the hybrid and dynamic methods and in Figure 5 for the fault-tree method.

The fault-tree model results in these cases do not immediately yield actionable information to design teams, as the LOM and LOC fault-trees respectively produced 900 and 3,956 cutsets of exact system failure modes, precisely capturing data about which components failed in what mode in the approximate system. For LOM, there exist only 24 unique classes of cutsets when the specificity of which exact component failed is removed. However, it is still difficult to directly apply the results in Figure 5 to provide actionable information to the design team.

Similarly, the results from the dynamic simulation method must also be processed. The frequency of failure of each component during a mission with a LOM outcome is shown in Figure 4. Both the frequency of failure and frequency of failure leading to a LOM provide actionable information to the designer as to what failure modes are driving the system risk. However, a drawback of the dynamic method is that the true frequencies of failure modes not observed during any of the simulation realizations remain somewhat uncertain. In this case, there were no observed failures of the isolation valves, even though this failure mode does show up in both the hybrid and fault-tree results.

The hybrid model immediately provides an ordered list of approximate risk drivers at the failure mode level as the approach neglects to model cross-component interactions. Since these cross-component cutsets do not drive the risk of the system, however, the primary risk drivers remain the same. Interestingly, the hybrid model predicts a much higher occurrence of valves failing leaky than both the fault-tree and dynamic methods. This is due to the conservative assumption that the diverse leak protection provided by the isolation valves must be reliable for the entire mission, since the existing ART model is not able to capture this dynamic behavior explicitly.

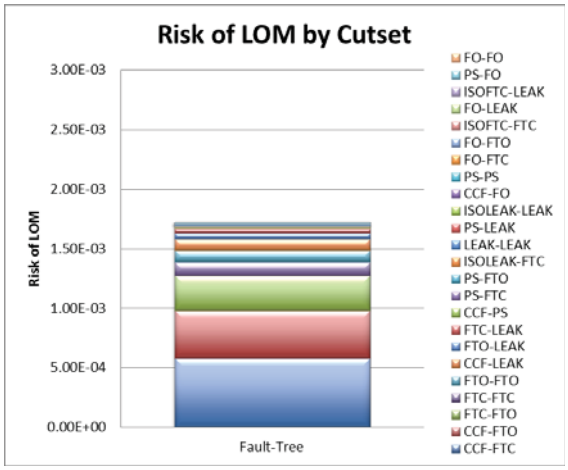



*Figure 4– System Risk of LOM by Failure Mode for the Fault-Tree Method*

Providing risk data at the failure-mode level can yield much richer insights into how system safety and reliability can be improved most efficiently. In this case, it is clear that the dominant failure modes of the system are Valve - Fails to Open and Valve - Fails to Close. The fault-tree results do benefit by providing the information that it is common cause failures of this failure mode that drive system risk. Thus, a designer would want to spend precious project resources, such as mass, to protect against this failure mode by backing up these functions redundantly or reducing the susceptibility of these components to common cause failures.

The comparative results presented here were driven by common cause failures of the fails-to-open and fails-to-close thruster failure modes. As such, it would be interesting to perform a sensitivity analysis of the results to changes in the common cause factors and demand failure probabilities of these risk drivers to determine the impacts on each method's risk estimates. In addition, uncertainty analysis could be

included for each methodology to further illustrate their advantages and limitations. Ideally, the system under consideration should be expanded to increase the scope and complexity of system interactions and dynamics to better reflect complex, real-world space systems.

## *4 DISCUSSION*

The applicability of each methodology to the different phases of system development can now be discussed in light of the benefits and drawbacks presented in the previous section.

The methodology selected during the conceptual design phase needs to respond rapidly to a changing design and provide accurate relative risk drivers with limited design detail. The methodology best suited to providing such insights is the rapid fault-tree hybrid approach. Interestingly, many of the limitations associated with the hybrid approach are minimized early in the system development life cycle because the precise design details about cross strapping and component connectivity are still yet to be determined. Moreover, the purpose of PRA during the conceptual design phase is to provide the design teams with increased insight to guide design decision. Thus, most PRA in this phase will be of a relative nature and a precise, absolute risk estimate is not as important as the relative differences between multiple, competing design options. Furthermore, at this phase of development, the PRA is often more concerned with reliability potential rather than 'as drawn' reliability.

As the design begins to mature, more precise insights are required to accurately discriminate between similar trade study options and identify the factors that can most efficiently reduce overall risk. Additionally, risk estimates must be provided to discriminate between design options in completely unrelated subsystems, so having accurate absolute risk estimates becomes of paramount importance. The design trades will also start to become more subtly nuanced and require precise representations of actual real-world system operation. To accomplish this, the level of design detail represented in the risk model must go beyond redundancy and nominal mission operations to include dynamic, time- and state-dependent system responses as well as diverse system capabilities. The dynamic methodology is best suited to this phase of development, as many risk-driving and risk-differentiating phenomena are not easily captured by static methods.

Ultimately, once the design has been finalized and the goal of the PRA is to provide design validation and requirement verification, more traditional, static fault-tree approaches may become as appropriate as the simulation method. At this point in the design cycle, the goal of the PRA is often to show that the system meets requirements or validate the design by exhaustively searching for unintended system failure modes or cutsets that are not intuitively obvious and are very easy for a fault-tree to discover. Thus, making overly conservative assumptions can be completely valid. Moreover, since the questions being asked of the PRA are much broader and less specific, the PRA does not have to provide decision makers with as much detailed insight in such a rapid fashion.

## *5 ACKNOWLEDGEMENTS*

The authors would like to acknowledge the support, review, and comments from their fellow Engineering Risk Assessment team members, Scott Lawrence, Samira Motiwala, Lorien Wheeler, Ted Manning, Ken Gee and Daryl Robertson at NASA Ames Research Center.

## *REFERENCES*

1. S. A. Motiwala, D. L. Mathias, C. J. Mattenberger, "*Conceptual Launch Vehicle and Spacecraft Design for Risk Assessment*", NASA/TM-2014-218366, NASA ARC, Moffett Field, CA, 2014.
2. J. Miller, J. Leggett, and J. Kramer-White, "*Design Development Test and Evaluation Considerations for Safe and Reliable Human Rated Spacecraft Systems*," NASA, 2008, Hampton, VA.
3. L. E. Booth, "*IEEE Guide to the collection and presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability data for nuclear-power generating stations,"* IEEE Std 500-1984, New York, NY, 1983.
4. Reistle, Bruce, Global Alpha Model Uncertainty Tool (GAMUT), July 2011.
5. Idaho National Laboratory (INL©), SAPHIRE®, Version 8, Idaho Falls, Idaho.
6. B. F. Putney, E. Tavernetti, J.R. Fragola, and E. Gold, "*Reliability Tool for a Preliminary Quantified Functional Risk and Hazard Analysis*," Proceedings of the Reliability and Maintainability Symposium, 2009, Fort Worth, TX.
7. www.goldsim.com
8. D. B. Kececioglu, "*Reliability Engineering Handbook, Volume 2*", DEStech Publications, Lancaster, PA, 2002.
9. https://aws.amazon.com/what-is-cloud-computing/
10. B. Rupak, "*A Look at the Impact of High-End Computing Technologies on NASA Missions*", ARC-E-DAA-TN4714, NASA Ames Research Center, 2012.
11. S. Go, D. L. Mathias, C. J. Mattenberger, S. Lawrence, K. Gee, "*An Integrated Reliability and Physics-based Risk Modeling Approach for Assessing Human Spaceflight Systems*," Probabilistic Safety Assessment and Management conference, 2014, Honolulu, HI.
12. MGL Reference
13. J. R. Fragola, "*Supporting Preliminary Design Decision Making with a Risk Data Base*," Proceedings of Probabilistic Safety Assessment and Management conference, 2010, Seattle, WA.
14. NUREG/CR-5485
15. NUREG/CR-5496

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

# Comparative Analysis of Static & Dynamic Probabilistic Risk Assessment

***Reliability and Maintainability Symposium 2015***

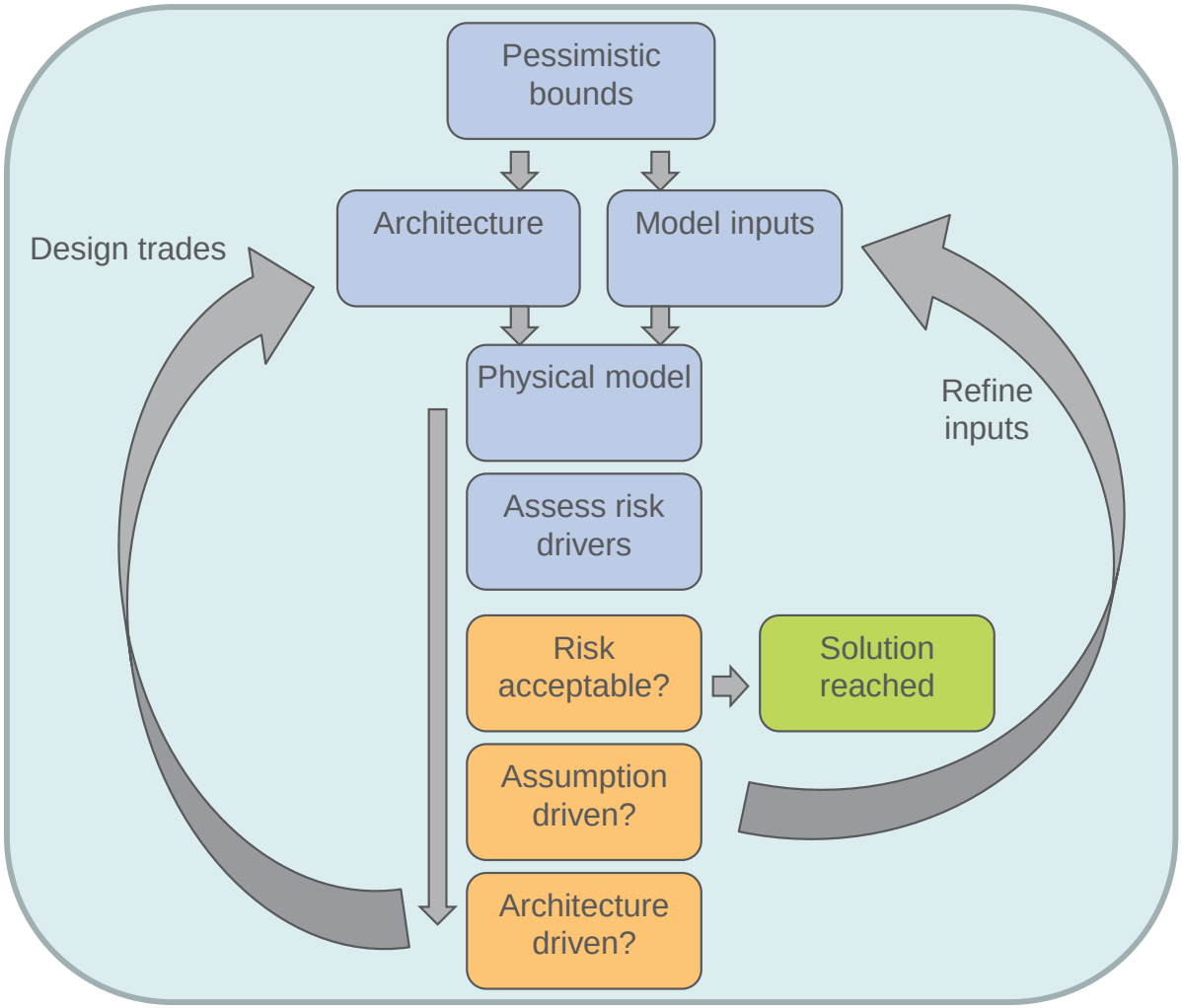

***Chris Mattenberger, Science & Technology Corporation***
***Donovan Mathias & Susie Go, NASA ARC***
***Engineering Risk Assessment Team***
***NASA Ames Research Center, Moffett Field, California***


***January 27th, 2015***

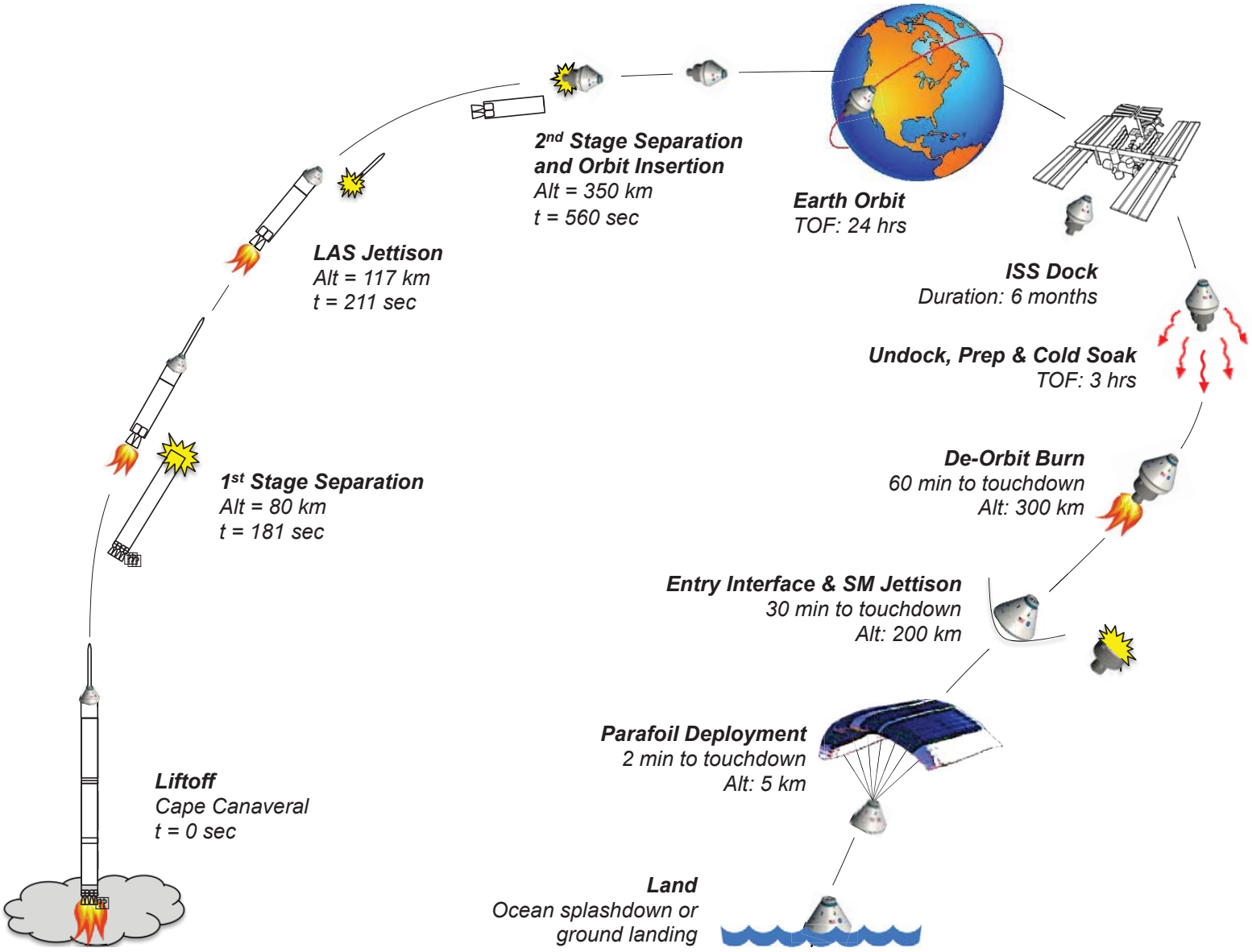
# Application of ERA Team Approach

- **Risk-informed decision support**
  - Requirement verification
  - Risk-informed design support
  - Part selection/procurement
- **Probabilistic risk assessment is informative, not predictive**
  - Provides quantitative answers to specific questions
  - Always driven by specific application
  - Based on traditional methods and extended as appropriate

**Iterative/responsive modeling approach**



# ERA Generic Launch Vehicle & Spacecraft



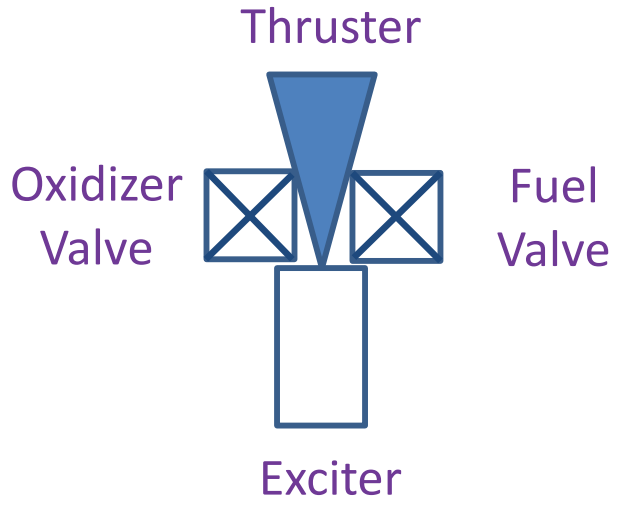

**Mission concept of operations used as comparative basis**

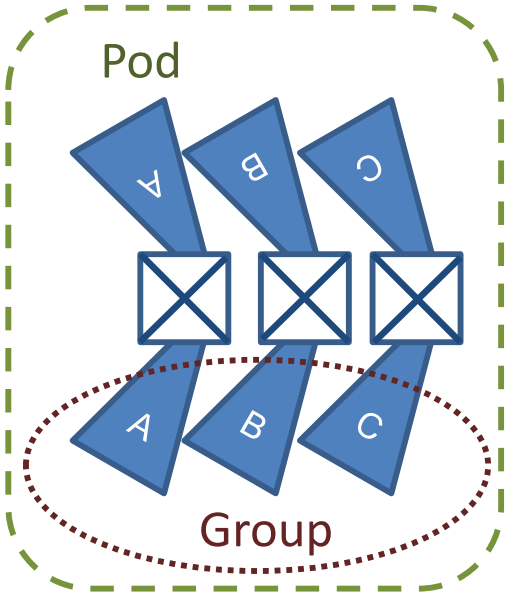
# Probabilistic Risk Assessment Scope

| Failure Mode | Failure Rate / Probability |
|---|---|
| Valve – Fails to Open | 2.05e-6 / demand |
| Valve – Fails to Close | 1.51e-6 / demand |
| Valve – Fails Operationally | 9.00e-7 / hour |
| Valve – Fails Leaky | 5.00e-8 / hour |
| Exciter – Fails Off | 1.69e-5 / hour |

| Common Cause Group Size | Common Cause Factor |
|---|---|
| CCF of 2 of 3 | 0.0483 |
| CCF of 3 of 3 | 0.00517 |

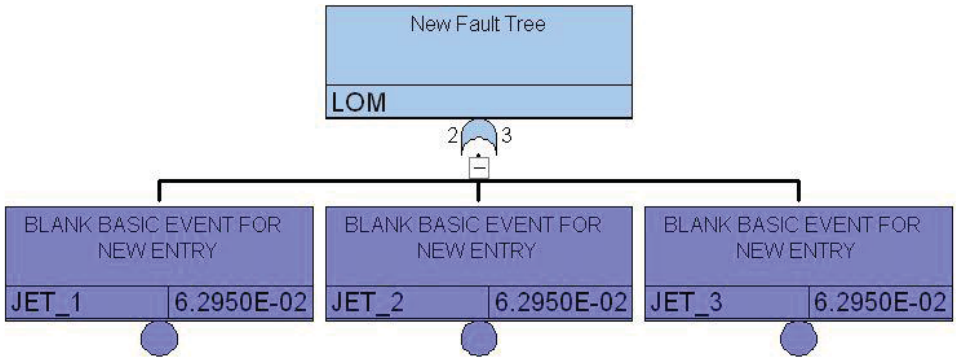
| Failure Mode | Pre-Docking | Docked | Post-Undock |
|---|---|---|---|
| Valve – Fails to Open | 2000 demands | N/A | 1000 demands |
| Valve – Fails to Close | 2000 demands | N/A | 1000 demands |
| Valve – Fails Operationally | 2 hours | N/A | 1 hours |
| Valve – Fails Leaky | 24 hours | 5040 hours | 4.5 hours |
| Exciter – Fails Off | 24 hours | N/A | 4.5 hours |



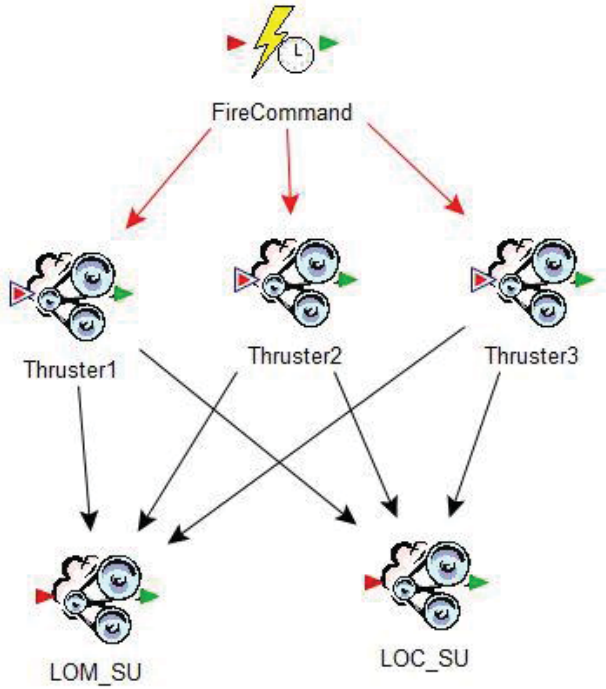




**Highly dynamic response to failures and highly interconnected peers**

# Methodologies




Fault-Tree



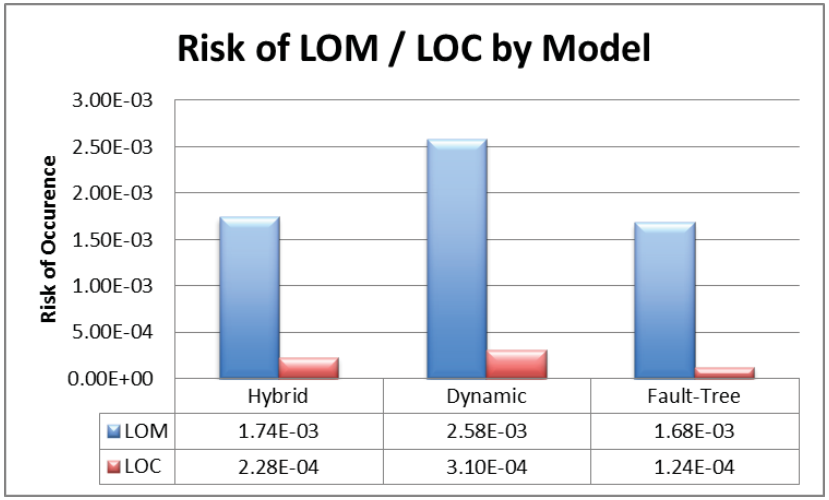

Dynamic

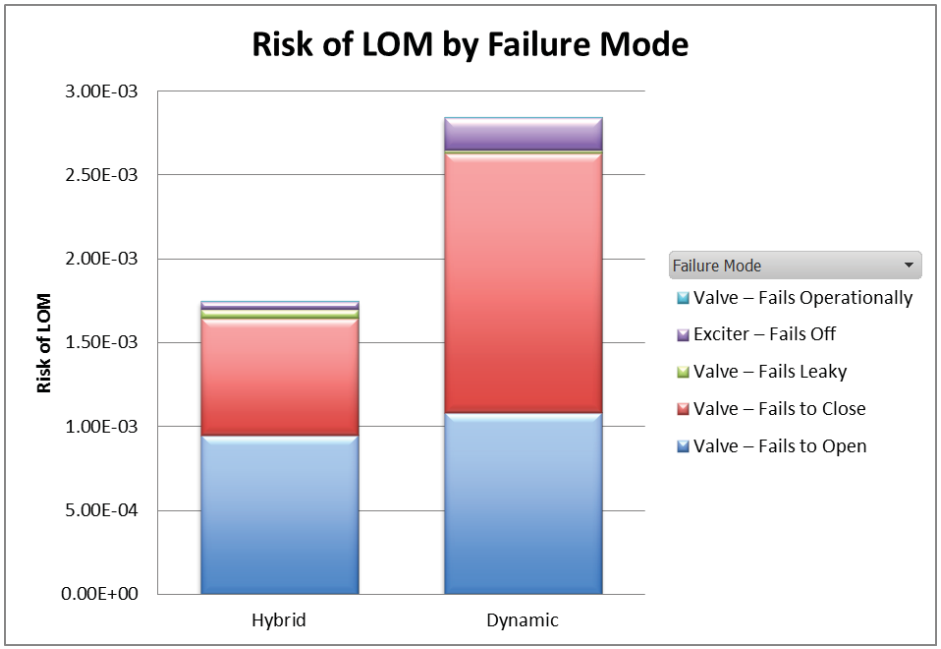
| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | AA | AE | AC | AD | AE | AF | AG |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | MEL Inputs | | | | | Failure Rate Data | | | | | | | | System Response to Failure | | | | | | | | Risk Exposure [hrs] | | | | | | | Risk Results | | | Reliability Results | |
| 2 | | | | | | | | | | | | | | | | | 4 | | | | | 0.1542 | 24 | 4366 | 26 | 3.5 | 0.5 | | 2.42E-02 | 9.23E-04 | | 9.76E-01 | 9.99E-01 |
| 3 | Subs | V | MEL Name | Mass | | Data Surrogate | Failure Ra | Units | Source | CCF2 | CCF3 | CCF4 | | HS | CS | Abort Threshold | Abort Time | LOC Threshold | DB LOM | DB LOC | | Ascent | Pre-Docking | Docked (Off) | Docked (On) | Post-Undock | EDL | | LOM | LOC | | LOM_Total | LOM_LOC |
| 173 | AVI | | Avionics | 342.6 | | | | | | | | | | | | | | | | | | | | | | | | | | | | 1.000E+00 | 1.000E+00 |
| 174 | AVI | | GNC | 53 | | | | | | | | | | | | | | | | | | | | | | | | | | | | 1.000E+00 | 1.000E+00 |
| 175 | AVI | | Sensor Monitor | 10 | | All - Not Credible Failure | 0.00E+00 | Hour | Assumption. Ra | 0.000 | 0.000 | 0.000 | | | | | | | | | | 0.1542 | 24 | 0 | 26 | 3.5 | 0.5 | | | | | 1.000E+00 | 1.000E+00 |
| 176 | AVI | | Integrated GPS/INS | 9.5 | | All - Integrated GPS/INS | 5.00E-05 | Hour | Honeywell SIGI | 0.030 | 0.007 | 0.004 | | | 1 | 1 | 4 | 0 | | 0.99 | | 0.1542 | 24 | 0 | 26 | 3.5 | 0.5 | | 2.51E-03 | 4.26E-07 | | 9.97E-01 | 1.000E+00 |
| 177 | AVI | | Integrated GPS/INS | 9.5 | | All - Cold Spare | 0.00E+00 | Hour | Assumption. Ra | 0.000 | 0.000 | 0.000 | | | | | | | | | | 0.1542 | 24 | 0 | 26 | 3.5 | 0.5 | | | | | 1.000E+00 | 1.000E+00 |
| 178 | AVI | | Star Tracker Package | 6 | | All - Star Tracker (CT-602) | 9.51E-06 | Hour | Ball Aerospace | 0.030 | 0.007 | 0.004 | | | 1 | 1 | 4 | 0 | | | | 0.1542 | 24 | 0 | 26 | 3.5 | 0.5 | | 4.78E-04 | 8.05E-06 | | 9.99E-01 | 1.000E+00 |
| 179 | AVI | | Star Tracker Package | 6 | | All - Cold Spare | 0.00E+00 | Hour | Assumption. Ra | 0.000 | 0.000 | 0.000 | | | | | | | | | | 0.1542 | 24 | 0 | 26 | 3.5 | 0.5 | | | | | 1.000E+00 | 1.000E+00 |
| 180 | AVI | | VNS LIDAR | 12 | | All - Non-Critical Failure | 0.00E+00 | Hour | Non-Critical Fai | 0.000 | 0.000 | 0.000 | | | | | | | | | | 0.1542 | 24 | 0 | 26 | 3.5 | 0.5 | | | | | 1.000E+00 | 1.000E+00 |

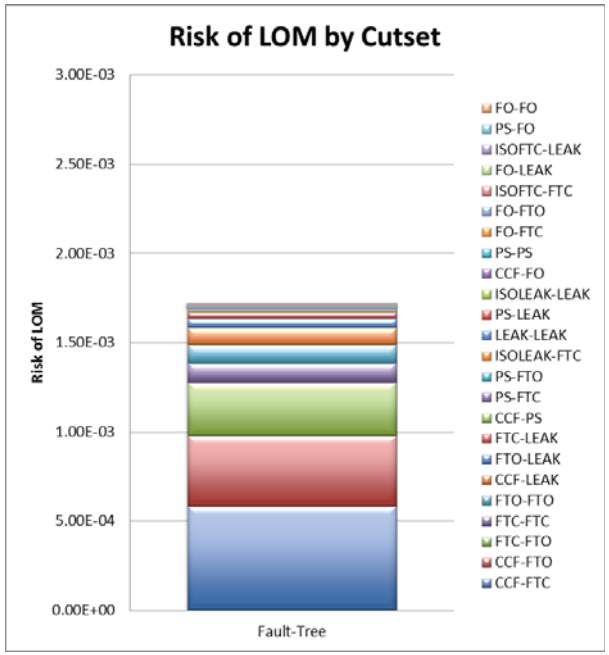
Hybrid

**Each approach provides solutions to approximate problems**

# Comparison of Results




**Risk model insights must provide actionable information to decision makers**

# System Life Cycle

- **Conceptual Design Phase**
  - Design evolves rapidly
  - Lack of precise design details
  - Trades performed at higher levels of design or architecture
  - Focus is on Reliability Potential
- **Preliminary Design Phase**
  - Design continues to evolve rapidly
  - Additional design details become available
  - Trades performed at lower levels of design or architecture
  - Trades must discriminate between closely related system options
  - Focus begins to shift from Reliability Potential to “As Drawn”
- **Critical Design Phase**
  - Design has begun to crystalize
  - Complete design details become available
  - Part selection, procurement, test plan enter trade space
  - Focus is entirely “As Drawn”
- **Operational Phase**
  - Real-world data about system available
  - Maintenance enters trade space
  - Real-time decision support
  - Focus is entirely “As Operated” and “As Built”

# Summary & Conclusions

- **Hybrid Approach**
  - Most well suited for conceptual and preliminary designs
  - Responds rapidly to changing design
  - Complete design details not necessary
  - Does not capture all system failure modes

- **Dynamic Approach**
  - Most well suited for preliminary, critical and operational designs
  - Provides greater design insights
  - Captures dynamic behavior
  - Captures interconnectivity and time- / state- dependencies among subsystems
  - Difficult to create new models and validate

- **Traditional Fault-Tree Approach**
  - Most well suited for critical designs
  - Allows for conservative assumptions to capture dynamics
  - Design has crystalized so it has a chance to keep up
  - Questions at this phase are higher level

# Q & A